



Building An 11 Node Raspberry Pi Cluster

Laquinn Nimmons
Voorhees College

Mentors
Matt Myrick & John Donaldson,
Lawrence Livermore National
Lab

Lawrence Livermore
National Lab



Abstract

Why build a cluster? There are many reasons why an individual would want to build a cluster. One reason I chose to build one was to explore parallel computing and how it could help certain aspects of cyber security.

In this presentation I will provide you with information about a cluster that was built from raspberry pi's. I will talk about what software I used to build and program the cluster.

Introduction

A **Beowulf cluster** is a cluster of computers networked into a small local area network with libraries and programs installed which allow processing to be shared among them. Beowulf is a multi-computer architecture, which can be used for parallel computations. It is a system that usually consists of one server node, and one or more client nodes connected via Ethernet or some other network. It is a system built using commodity hardware components, Unix-like operating system, with standard Ethernet adapters, and switches. The server node controls the whole cluster and serves files to the client nodes. It is also the cluster's console and gateway to the outside world.

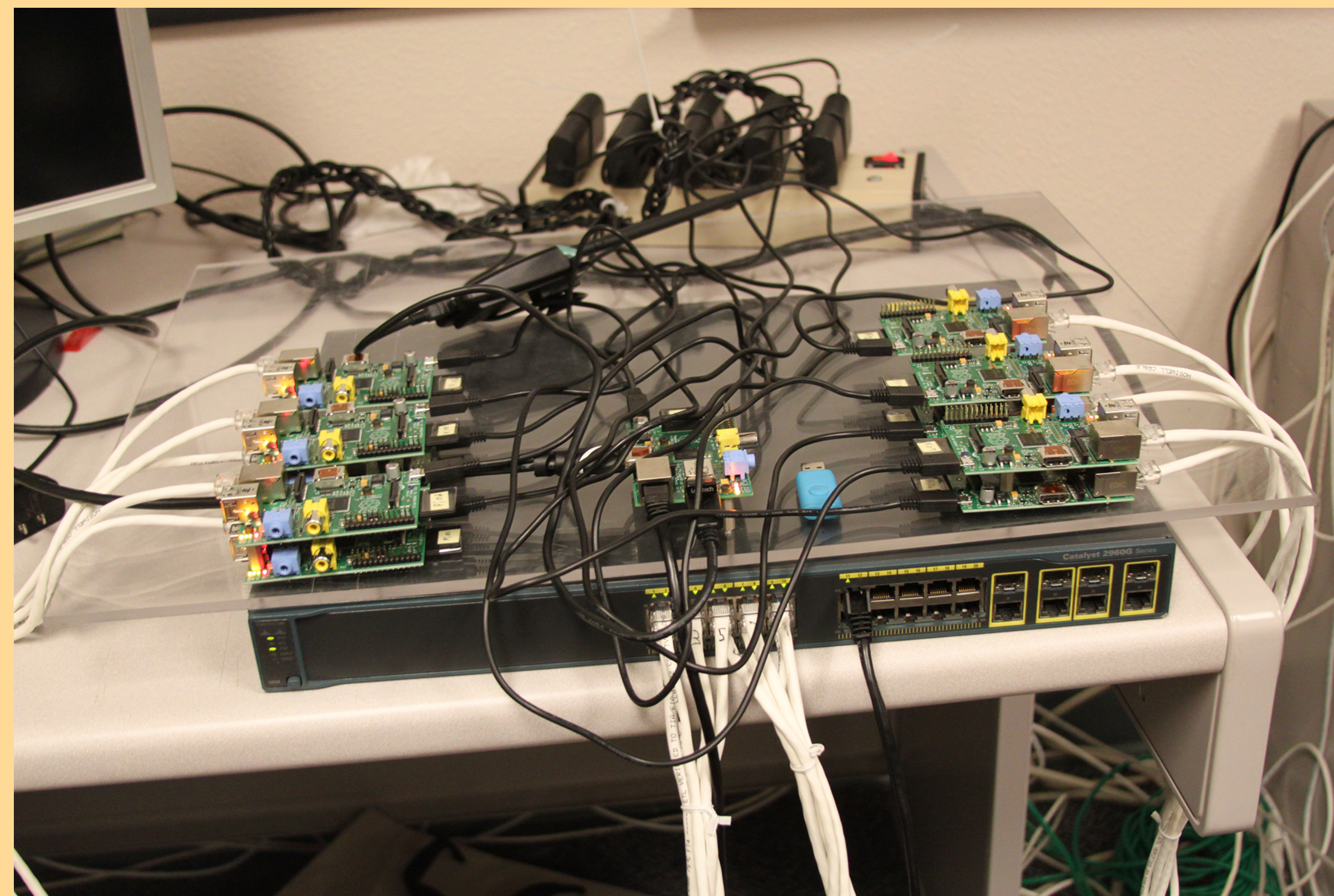
Equipment

This is a list of what you will need to build the Raspberry pi
“Beowulf” cluster

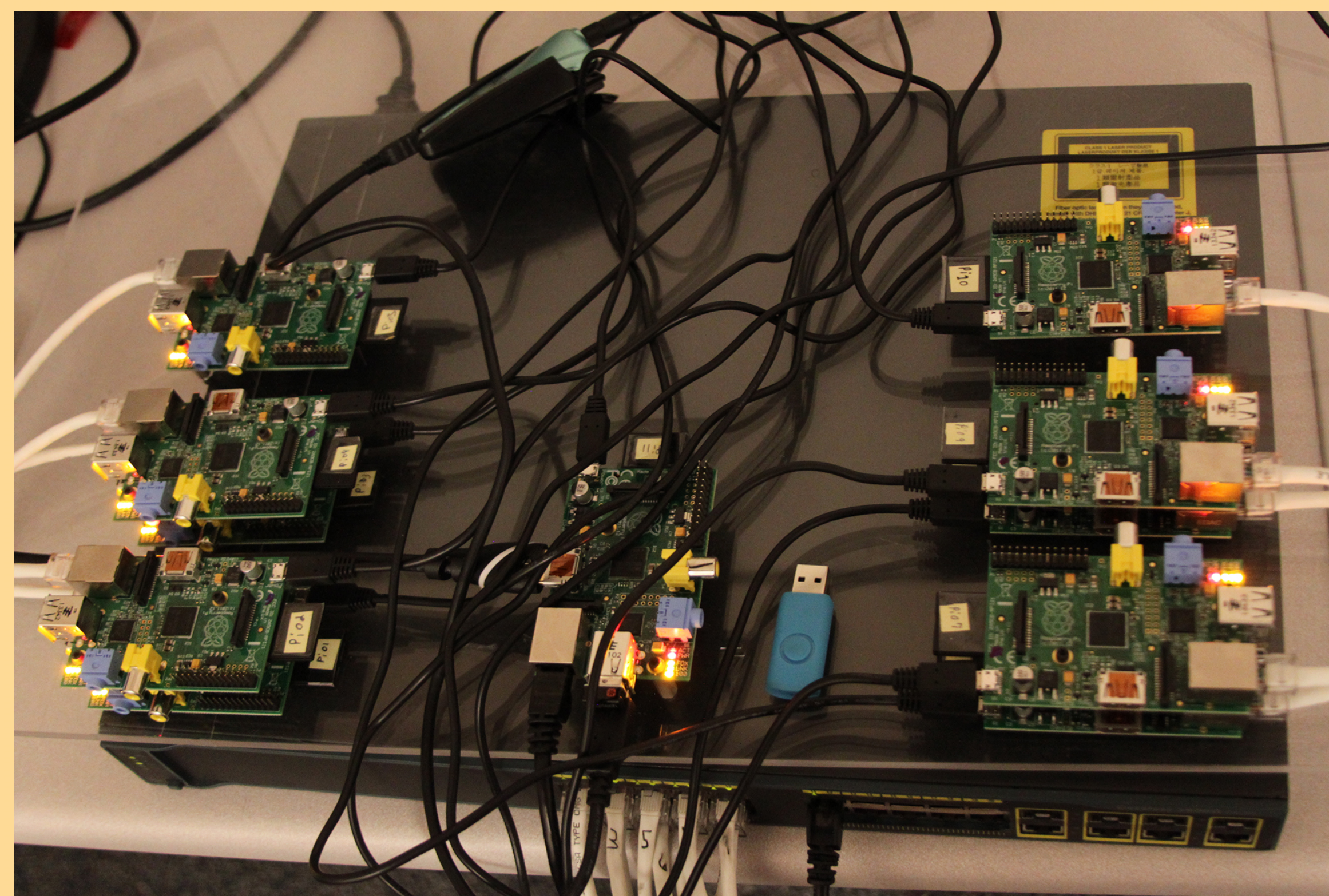
- Raspberry Pi Model B (11)
- 16 GB Class 10 SD card (11)
- Ethernet cables (11)
- Micro usb power cable (11)
- Keyboard/Mouse (1)
- Wireless Dongle (1)
- 13 outlet surge protector (1)
- Monitor with DVI connection (1)
- HDMI cable\ with DVI extension (1)
- A switch or hub at least 11 ports (1)
- 24” by 16” plastic sheet .25” thick (1)
- Mounting screws and nuts (14 of each)

Software

- **MPI**, the Message Passing Interface, is a standardized and portable message-passing system designed to function on a wide variety of parallel computers. The standard defines the syntax and semantics of library routines and allows users to write portable programs in the main scientific programming languages (Fortran, C, or C++).
 - MPICH2
- **gfortran** is the name of the GNU Fortran compiler, which is part of the GNU Compiler Collection (GCC).
 - Gfortran
- **Python libraries** had to be installed to run some test files.



The pictures that are above and below this caption is the final build of the 11 node Raspberry pi Cluster.



References

- <http://www.tinkernut.com/2014/04/27/make-cluster-computer/>
- <http://en.wikipedia.org/wiki/Gfortran>
- http://en.wikipedia.org/wiki/Beowulf_cluster

Dictionary attack

A dictionary attack is a technique or method used to breach the computer security of a password-protected machine or server. A dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password or trying to determine the decryption key of an encrypted message or document.

Dictionary attacks are often successful because many users and businesses use ordinary words as passwords. These ordinary words are easily found in a dictionary, such as an English dictionary.

Results

After the final build I used a modified version of a python program to crack md5 hashes using the Dictionary attack.

```
Mpiexec -f machinefile -n 11 python python_test/md5_attack.py
```

```
I am process 9 of 11 on pi10 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 8 of 11 on pi09 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 6 of 11 on pi07 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 1 of 11 on pi02 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 3 of 11 on pi04 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 4 of 11 on pi05 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 7 of 11 on pi08 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 5 of 11 on pi06 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 0 of 11 on pi01 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 2 of 11 on pi03 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
I am process 10 of 11 on pi11 and i have successfully cracked the hash c80cc0537e6c13e09a296dd19594aea0: It's tiger123
```

This file is to show how the hash was crack with multiple processes.

Conclusion/ Further work

To recap on the information provided in the poster this project was building a cluster with 11 raspberry pi's then programing them to be able to commutate with each other. This project introduced me to parallel programming and how it works with the the computers that are networked together and to all run in parallel with each other.

Passwords are important in present time and as a computer user we should know what a strong password looks like so we can protect ourselves better from adversaries that are trying to get them and do wrong with them..

For further research on this topic I would like to learn more about parallel programming and how we can use it with in Cyber security to increase the protection of networks and data.